AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

and Limited Official Use documents may be reproduced to the extent required by operational needs.

(c) Reproductions of classified documents shall be subject to the same accountability and controls as the original documents.

(d) Paragraphs (a) and (b) of this section shall not restrict the reproduction of documents to facilitate review for possible declassification.

§ 2.32 Loss or possible compromise [4.1(b)].

(a) *Report of Loss or Possible Compromise.* Any Treasury employee who has knowledge of the loss or possible compromise or classified information shall immediately report the circumstances to their designated office or bureau security officer who shall take appropriate action to assess the degree of damage. In turn, the Departmental Director of Security shall be immediately notified by the affected office or bureau security officer of such reported loss or possible compromise. The Departmental Director of Security shall also notify the department or agency which originated the information and any other interested department or agency so that a damage assessment may be conducted and appropriate measures taken to negate or minimize any adverse effect of the loss or possible compromise. Compromises may occur through espionage, unauthorized disclosures to the press or other members of the public, publication of books and treatises, the known loss of classified information or equipment to foreign powers, or through various other circumstances.

(b) *Inquiry.* The Departmental Director of Security shall notify the Assistant Secretary (Management) who shall then direct an immediate inquiry to be conducted for the purpose of taking corrective measures and assessing damages. Based on the results of this inquiry, it may be deemed appropriate to notify the Inspector General who shall determine whether the Office of the Inspector General or a Treasury bureau will conduct any additional investigation. Upon completion of the investigation by the Inspector General, the Inspector General shall recommend to the Assistant Secretary (Management) and concurrently to the Departmental Director of Security, the appropriate administrative, disciplinary, or legal action to be taken based upon jurisdictional authority of the Treasury components involved.

(c) *Content of Damage Assessments.* At a minimum, damage assessments shall be in writing and contain the following:

(1) Identification of the source, date and circumstances of the compromise.

(2) Classification and description of the specific information which has been lost.

(3) An analysis and statement of the known or probable damage to the national security that has resulted or may result.

(4) An assessment of the possible advantage to foreign powers resulting from the compromise.

(5) An assessment of whether,

(i) The classification of the information involved should be continued without change;

(ii) The specific information, or parts thereof, shall be modified to minimize or nullify the effects of the reported compromise and the classification retained;

(iii) Downgrading, declassification, or upgrading is warranted, and if so, confirmation of prompt notification to holders of any change, and

(6) An assessment of whether countermeasures are appropriate and feasible to negate or minimize the effect of the compromise.

(d) *System for Control of Damage Assessments.* Each Treasury bureau and the Departmental Offices shall establish a system of control and internal procedures to ensure that damage assessments are performed in all cases described in § 2.32(a) and that records are maintained in a manner that facilitates their retrieval and use within the Department.

(e) *Cases Involving More Than One Agency.* (1) Whenever a compromise involves the classified information or interests of more than one agency, the Departmental Director of Security shall advise the other affected agencies of the circumstances and findings that affect their information or interests. Whenever a damage assessment, incorporating the product of two or more

agencies is needed, the affected agencies shall agree upon the assignment of responsibility for the assessment and Treasury components will provide all data pertinent to the compromise to the agency responsible for conducting the assessment.

(2) Whenever a compromise of United States classified information is the result of actions taken by foreign nationals, by foreign government officials, or by United States nationals in the employ of international organizations, the agency performing the damage assessment shall endeavor to ensure through appropriate intergovernmental liaison channels, that information pertinent to the assessment is obtained. Whenever more than one agency is responsible for the assessment, those agencies shall coordinate the request prior to transmittal through appropriate channels.

(3) Whenever an action is contemplated against any person believed responsible for the loss or compromise of classified information, damage assessments shall be coordinated with appropriate legal counsel. Whenever a violation of criminal law appears to have occured and a criminal prosecution is contemplated, coordination shall be made with the Department of Justice.

(4) The designated representative of the Director of Central Intelligence, or other appropriate officials with responsibility for the information involved, will be consulted whenever a compromise of sensitive compartmented information has occurred.

§ 2.33 Responsibilities of holders [4.1(b)].

Any person having access to and possession of classified information is responsible for protecting it from persons not authorized access, i.e., persons who do not possess an appropriate security clearance, and who do not possess the required need-to-know. This includes keeping classified documents under constant observation and turned facedown or covered when not in use and securing such information in approved security equipment or facilities whenever it is not under the direct supervision of authorized persons. In all instances, such protective means must meet accountability requirements prescribed by the Department.

§ 2.34 Inspections [4.1(b)].

Individuals charged with the custody of classified information shall conduct the necessary inspections within their areas to ensure adherence to procedural safeguards prescribed to protect classified information. Security officers shall ensure that periodic inspections are made to determine whether procedural safeguards prescribed by this regulation and any bureau implementing regulation are in effect at all times. At a minimum such checks shall ensure that all classified information is stored in approved security containers, including removable storage media, e.g., floppy disks used by word processors that contain classified information; burn bags, if utilized, are either stored in approved security containers or destroyed; and classified shorthand notes, carbon paper, carbon and plastic typewriter ribbons, rough drafts and similar papers have been properly stored or destroyed.

§ 2.35 Security violations.

Any individual, at any level of employment, determined to have been responsible for the unauthorized release or disclosure or potential release or disclosure of classified national security information, whether it be knowingly, willfully or through negligence, shall be notified on TD F 71–21.1 (Record of Security Violation) that his or her action is in violation of this regulation, the Order, the Directive, and Executive Order 10450, as amended. Treasury Directive 71–04, entitled, ''Administration of Security Violations'' sets forth provisions concerning security violations which shall apply to each Treasury employee and persons under contract or subcontract to the Department authorized access to Treasury classified national security information.

(a) Repeated abuse of the classification process, either by unnecessary or over-classification, or repeated failure, neglect or disregard of established requirements for safeguarding classified information by any employee shall be